REMARKS/ARGUMENTS

I. Introduction:

Claims 1, 6, and 23 are amended. With entry of this amendment, claims 1, 3, 4, 6-7, 9, 16, 18-20, and 23 will be pending.

The courteous telephone interview granted applicants' undersigned attorney by Examiner Boutah on September 18, 2006 is hereby respectfully acknowledged. The arguments presented to Examiner Boutah in the interview are set forth below.

II. Claim Rejections Under 35 U.S.C. 101:

The specification has been amended to specify that a carrier wave (e.g., in a network including the Internet) is an example of a transmission medium. Claims 6, 7, and 9 are therefore limited to statutory subject matter and are believed to comply with the requirements of 35 U.S.C. 101.

III. Claim Rejections Under 35 U.S.C. 103:

Claims 1, 3, 4, 6, 7, 9, 16, 18-20, and 23 stand rejected under 35 U.S.C. 103 as being unpatentable over U.S. Patent No. 6,754,706 (Swildens et al.) in view of U.S. Patent Nos. 6,735,631 (Oehrke et al.) and 6,665,702 (Zisapel et al.).

Applicant respectfully submits that the pending claims are patentable over Swildens et al., Oehrke et al. and Zisapel et al.

The Swildens et al. patent discloses a scalable domain name system. As shown in Fig. 3, Swildens et al. perform the following steps at a DNS server upon receiving a request from a client DNS server: (1) check to see if the client is part of group that the server is authoritative; (2) if the server is not authoritative, the request is forwarded to the proper server and no persistence check is performed; (3) if the server is authoritative, it is determined if a persistent response is required; and (4) if a persistent response is required, the persistent entry is sent to the requestor.

Swildens et al. do not show or suggest determining if a local director has received and sent out connection requests from any client having the same natural class as a first client by identifying previous connections and selecting the same server for connection, if the local director has received and sent out a connection request, as set forth in the independent claims.

Swildens et al. use authoritative connections to identify a group of servers associated with a group of clients. If the server receiving the request is not authoritative, the server simply forwards the request to an authoritative server. If a server receiving a request is authoritative, the server performs a conventional persistence check to see if a persistent connection is required. If a persistence connection is required, a table containing the client IP address and hostnames is checked and the specific IP address for that persistent connection is provided. It is important to note that the method disclosed by Swildens et al. does not solve the problem addressed by applicant's invention. That is, there are situation, where a client IP address will change, thus, using the IP address to provide a persistent connection will not work. For example, a firewall may translate the network address into one or more IP addresses managed by the firewall. Conventional source persistence, as used by Swildens et al., will not work in situations where the user's IP address changes, such as when the user resides behind a firewall or array of firewalls that use multiple IP addresses.

In contrast to Swildens et al, and the cited references, Applicant's invention implements a sticky connection despite the presence of a firewall or other network device that may modify a client IP address, by checking to see if the local director has received and sent out connection requests from the client sending the request or any client having the same natural class as the first client.

Swildens et al. consult a table to determine if a persistent entry exists that ties a machine IP address and hostname to an IP address. For persistent hostnames, when a DNS request comes in from a client, the DNS server checks its persistent table to see if there is a persistency entry. If there is, the server will return the persistent IP address. The persistent connection is only provided for a single IP address mapped to a client. When a request having a persistence connection is received, the DNS server merely returns the same IP address for subsequent requests. In contrast to Applicant's claimed invention, the server of Swildens et al. does not determine if connection requests have previously been received from any client have the same natural class. If the client address changes, due to the firewall example discussed above, the entry will not be found in the table and persistent connection will be lost. Thus, Swildens et al. do not show or suggest selecting the same server for connection with a client if the DNS server has previously received and sent out a connection request from any client having the same natural class.

Furthermore, Swildens et al. do not show or suggest selecting a real server based on load balancing if the local director has not received and sent out a connection request to one of the servers. Swildens et al. only perform load balancing among authoritative servers. If the DNS server receiving the request for an IP address is authoritative, then a response is sent and no load balancing is performed. Applicant's invention, as set forth in claim 1, allows for load balancing among all servers in communication with a local director if the local director has not received and sent out a connection request to one of the real servers from any client having the same natural class as the client. Applicant's invention is particularly advantageous in that if a client having a natural class for which no connection has been made requests a connection, a server can be selected based strictly on load balancing with no concern for selecting an authoritative server. Also, since connections are identified in a table stored on the local director, sticky connections can be timed out after a specified period for one or more natural classes.

As noted by the Examiner, Swildens et al. do not teach selecting the same server for all clients having the same natural class subnet. The Examiner cited Zisapel et al. with regard to this limitation.

Zisapel et al. disclose load balancing client requests among redundant network servers in different geographical locations. The method includes directing requests from a source to a subnet that is the same as the subnet of the requester to the closest load balancer. The load balancer identifies the best server farm sites to which requests from a particular subnet should be routed. Each server farm comprises a plurality of servers to which the load balancer may send a request (see, for example, Fig. 1A). Zisapel thus only selects a load balancer and server farm site based on the subnet of the requester and since different servers can be selected, Zisapel teaches away from using persistent connections.

Oehrke et al. is directed to a method and system for networking redirecting, and does not remedy the deficiencies of the primary reference.

Accordingly, claim 1 is submitted as patentable over Swildens et al. and Oehrke et al. Claims 3-4 and claims 18-20, depending directly from claim 1, are submitted as patentable for the same reasons as claim 1.

With regard to claim 3, Swildens et al. do not address receiving a request from a firewall. In rejecting claim 3, the Examiner refers to col. 6, lines 46-65. This section of the patent refers to how latency probes send latency results only to DNS servers that need latency information for a given group. As discussed above, a firewall may translate the network address into one or more IP addresses managed by the firewall. In this case, the entry will not be found in the table described in Swildens et al, and the persistent connection will be lost.

Claim 18 is submitted as patentable over Swildens et al. because they do not show or suggest updating a table each time a connection is made between a local director and real servers with a new natural class. Swildens et al. are not concerned with tracking connections based on class since they select servers based on whether they are authoritative for a client DNS server.

Since Swildens et al. do not select servers based on a subnet mask, claim 19 is also further submitted as patentable over Swildens et al.

Claim 6 is a directed to a computer program product and claim 23 is directed to a system for providing a persistent connection between a client and a real server. Claims 6 and 23 are submitted as patentable for the reasons discussed above with respect to claim 1.

Claim 7-9, depending either directly or indirectly from claim 6, are submitted as patentable for the same reasons as claim 6.

IV. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,

Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-399-5609